デジタル社会推進標準ガイドライン DS-910

# 安全保障等の機微な情報等に係る政府情報システムの取扱い（案）

2022 年（令和４年）12 月 XX 日
デジタル社会推進会議幹事会決定

〔ガイドライン〕
規範として順守するドキュメント

〔キーワード〕
機微な情報、自律性、クラウドサービス

〔概要〕
安全保障等の機微な情報等を扱う情報システムについて、注意が必要とされるリスクとその対応策、クラウド化の検討、データ連携における留意点といった、利用者が検討すべき観点をまとめた標準ガイドライン附属文書。

## 改定履歴

| 改定年月日 | 改定箇所 | 改定内容 |
|---|---|---|
| 2022年X月X日 | - | 初版決定 |

# 目次

## １　基本的考え方

安全保障、公共の安全・秩序の維持といった機微な情報及び当該情報になり得る情報[1]を扱う情報システムにおいては、情報システムの停止や情報漏えい等による社会的影響は計り知れないため、そうした情報を扱う者自らの説明責任が特に強く求められている。そのため、情報システムの利用に当たっては、機器構成や設置場所、運用体制等を利用者自らが把握できることや運用面のガバナンスを利かせられること等、利用者にとっての高度な自律性が重視される。

[1]行政文書の管理に関するガイドライン（内閣総理大臣決定。初版平成 23 年 4 月 1 日。）に掲げる秘密文書中秘文書に該当する情報及びそれに準ずる情報のこと。例えば以下の情報などが考えられるが、これらには経済安全保障に関連する重大な企業情報や先端的技術情報等も含み得るなど、我が国を取り巻く内外の情勢変化を十分に踏まえて解釈するものとする。
一　アクセスを認められた者以外の者が当該情報にアクセスすることにより、国の安全に損害を与えるおそれがある情報となり得るもの
二　アクセスを認められた者以外の者が当該情報にアクセスすることにより、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあると認められる情報のうち、特に慎重な取扱いが求められるもの
三　アクセスを認められた者以外の者が当該情報にアクセスすることにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがあると認められる情報

## 2　注意が必要なリスクとその対応策

安全保障等の機微な情報等を情報システム上で扱う場合には、運用者の不正によりデータが漏えい・改ざんされるリスク、情報システムが停止しても状況把握に時間がかかるリスク、ソフトウェアに不正な処理が混入するリスク、ハードウェアの調達が困難になるリスク、ハードウェアにネットワークアクセスできなくなるリスク等に対応する必要がある。このため、情報システムを構成する要素（データ、運用、ソフトウェア、ハードウェア、データセンタ・通信）ごとに、機密性・完全性・可用性の観点から、利用者が必要な項目を確認し、対策を講じることが重要である。講じることが必要と考えられる対策の観点は、以下のとおり。

情報システムの利用者は、取り扱う情報の社会的影響やコスト等を踏まえ、高度な自律性確保のためにどういった項目を求めるか、各項目をどういった水準で求めるかを検討し、調達を行うことが適切である。

表　2－1　情報システムを構成する要素と講じる対策の観点

| 構成要素 | 講じる対策の観点 |
|---|---|
| データ | ・　操作権限の制限<br>・　データの暗号化<br>・　データの削除<br>・　データの冗長性確保　等 |
| 運用 | ・　運用体制・人員の適正化<br>・　運用状況の記録・提供・監査<br>・　障害時対応　等 |
| ソフトウェア | ・　ソフトウェアの信頼性管理<br>・　ソフトウェアの脆弱性対応<br>・　ソフトウェアのメンテナンス対応　等 |
| ハードウェア | ・　ハードウェアの信頼性管理<br>・　ハードウェアの脆弱性対応　等 |
| データセンタ・通信 | ・　設置場所の適正化<br>・　データセンタ・通信の信頼性管理<br>・　データセンタ・通信の冗長性確保　等 |

## ３　クラウド化の検討

サービスが即座に利用できることや、リソースがスピーディーに拡張できること等の利便性を利用者が享受できることを背景に、政府情報システムにおいても、「クラウド・バイ・デフォルト原則」の下、安全保障等の機微な情報等を扱う情報システムも含め、クラウド化を検討していくことが求められる。

クラウド化のメリットを享受するためには、NIST の定義[2]等を踏まえると、基本的な要件として、オンデマンド・セルフサービス、ネットワーク経由の利用、リソース共用[3]、スピーディーな拡張性、計測可能なサービス及びマネージドサービスであることを求めるべきだと考えられる。

安全保障等の機微な情報等を扱う情報システムにおいてもクラウド化を進める場合には、こうしたクラウド化の特長を生かしつつ、２で述べた高度な自律性を確保していくことが重要になる。

## ４　データ連携における留意点

クラウド化の特長を生かしつつ、高度な自律性を確保していくためには、クラウドを含む複数の情報システムを組み合わせて利用する形態も想定される。その際に利用する情報システムは、自律性確保の度合いが異なる可能性があり、また複数の情報システムを連携させる場合には、脆弱性が発生しやすくなるため、十分に注意してデータ連携を行うことが必要である。特に、各々がデータを保存するのか否か、データを処理するのか否か、の観点から必要な対策を講じるべきである。

---

[2] National Institute of Standards and Technology, Special Publication 800-145, The NIST Definition of Cloud Computing

[3] クラウドとしてはリソース共用できる機能を有するが、重要情報の物理的削除等の自律性要件を求めた場合には、結果的に、利用者にとってリソース専用型となる可能性がある。